Title (en)

FULLY HOMOMORPHIC MESSAGE AUTHENTICATION METHOD, DEVICE AND SYSTEM

Title (de)

VERFAHREN, VORRICHTUNG UND SYSTEM ZUR VOLLSTÄNDIG HOMOMORPHEN NACHRICHTENAUTHENTIFIZIERUNG

Title (fr)

PROCÉDÉ, DISPOSITIF ET SYSTÈME D'AUTHENTIFICATION DE MESSAGE ENTIÈREMENT HOMOMORPHE

Publication

EP 3163792 A4 20180228 (EN)

Application

EP 15775600 A 20150209

Priority

- CN 201410309571 A 20140630
- CN 2015072570 W 20150209

Abstract (en)

[origin: US2016119346A1] Embodiments of the present disclosure provide a method, an apparatus, and a system for authenticating a fully homomorphic message, where the method includes: acquiring a message authentication key, where: the message authentication key includes a public key, a first character string, and a second character string; the first character string is a character string that consists of 0 and 1 and has a length of n; the second character string is a character string that consists of 0 and 1 and has a length of n; generating an authentication fingerprint corresponding to each bit of to-be-computed data; sending a computation request to a server; receiving an authentication fingerprint corresponding to the computation result; and performing correctness authentication on the computation result according to the received authentication fingerprint, which effectively reduces an amount of computation in a verification process.

IPC 8 full level

H04L 9/32 (2006.01)

CPC (source: EP US)

H04L 9/008 (2013.01 - EP US); **H04L 9/32** (2013.01 - US); **H04L 9/3231** (2013.01 - EP US); **H04L 63/0876** (2013.01 - US); **H04L 63/123** (2013.01 - US); **H04L 63/126** (2013.01 - EP US); H04L 63/0442 (2013.01 - EP US); H04L 63/0861 (2013.01 - EP US)

Citation (search report)

- [XA] FENG YANSHENG ET AL: "Secure and Verifiable Outsourcing of Sequence Comparisons", 25 March 2013, NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 243 - 252, ISBN: 978-3-540-76785-5, ISSN: 0302-9743, XP047388578
- [A] HENRY CARTER GEORGIA INSTITUTE OF TECHNOLOGY CARTERHCHIATECH EDU PATRICK TRAYNOR GEORGIA INSTITUTE OF TECHNOLOGY TRAYNORGAMMAC GAT: "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices", USENIX,, 14 August 2013 (2013-08-14), pages 1 - 16, XP061014449
- [A] SEBASTIAN FAUST ET AL: "Outsourced Pattern Matching", 8 July 2013, AUTOMATA, LANGUAGES, AND PROGRAMMING, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 545 - 556, ISBN: 978-3-642-39211-5, XP047035371
- [T] CRAIG GENTRY: "A FULLY HOMOMORPHIC ENCRYPTION SCHEME", 1 September 2009 (2009-09-01), XP055389118, Retrieved from the Internet <URL:https://crypto.stanford.edu/craig/craig-thesis.pdf> [retrieved on 20170707]
- [X] BARBOSA M ET AL: "Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20110829:142617, 29 August 2011 (2011-08-29), pages 1 - 29, XP061005208
- [A] BUGIEL SVEN ET AL: "Twin Clouds: Secure Cloud Computing with Low Latency", 19 October 2011, NETWORK AND PARALLEL COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CHAM, PAGE(S) 32 - 44, ISBN: 978-3-642-01969-2, ISSN: 0302-9743, XP047423166
- [A] CRAIG GENTRY ET AL: "Implementing Gentry's Fully-Homomorphic Encryption Scheme", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20110204:192637, 4 February 2011 (2011-02-04), pages 1 - 29, XP061004402
- [A] DARIO FIORE ET AL: "Efficiently Verifiable Computation on Encrypted Data", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20140609:022756, 9 June 2014 (2014-06-09), pages 1 - 42, XP061016238, DOI: 10.1145/2660267.2660366
- See references of WO 2016000453A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

US 10009343 B2 20180626; **US 2016119346 A1 20160428**; CN 105337736 A 20160217; CN 105337736 B 20181030; EP 3163792 A1 20170503; EP 3163792 A4 20180228; EP 3163792 B1 20190828; WO 2016000453 A1 20160107

DOCDB simple family (application)

US 201514985883 A 20151231; CN 201410309571 A 20140630; CN 2015072570 W 20150209; EP 15775600 A 20150209